NOTICE OF ALLOWANCE

1. The After Final amendment, received on 16 April 2009, has been entered into record. In this amendment, claims 11-13, 15, 16, 18-22, and 27-30 have been cancelled.

2. Claims 4-10 are presented for examination.

Response to Arguments

3. With regards to the objection to the drawings, the applicant has submitted amendments, and the examiner hereby withdraws the objection.

Allowable Subject Matter

4. Claims 4-10 are allowed.

The following is an examiner's statement of reasons for allowance:

As to claim 4, it was not found to be taught in the prior art of providing the Montgomery square of a secret number to a verifier, computing the Montgomery square of a random number and transmitting it to the verifier, selecting a challenge value from a set of {0,1} and sending it to the prover, computing $y = r \times_m s^e$ and sending y to the verifier, and checking the authenticity of the response.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Boscher et al. (US 2008/0130870 A1) discloses a system and method for processing data for the implementation of cryptographic algorithms using Montgomery operations.

b. Crandall et al. (US 2006/0174126 A1) discloses a system and method for device verification using fast elliptic encryption.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431